FortiManager - Release Notes

Version 6.4.8

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 14, 2022
FortiManager 6.4.8 Release Notes
02-648-800018-20221214

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-05-03	Initial release.
2022-05-04	Updated Resolved Issues on page 33 and Known Issues on page 47.
2022-05-06	Updated Known Issues on page 47.
2022-05-24	Updated Known Issues on page 47.
2022-05-26	Updated Known Issues on page 47.
2022-06-13	Updated Known Issues on page 47.
2022-06-29	Updated Resolved Issues on page 33 and Known Issues on page 47.
2022-08-17	Updated Known Issues on page 47.
2022-10-20	Added 765709 to Resolved Issues on page 33.
2022-11-21	Updated Known Issues on page 47.
2022-12-01	Updated FortiGate models on page 22.
2022-12-14	Updated Known Issues on page 47.

FortiManager 6.4.8 Release

This document provides information about FortiManager version 6.4.8 build 2473.

The recommended minimum screen resolution for the FortiManager GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

Supported models

FortiManager version 6.4.8 supports the following models:

FortiManager	FMG-200F, FMG-200G, FMG-300E, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, FMG-3900E, and FMG-4000E.
FortiManager VM	FMG-VM64, FMG-VM64-Ali, FMG-VM64-AWS, FMG-VM64-AWSOnDemand, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see FortiManager VM firmware on page 13.

See also Appendix B - Default and maximum number of ADOMs supported on page 51.

You can use the FortiManager VM subscription license with new FMG-VM installations.

For existing FMG-VM installations, you cannot upgrade to a FortiManager VM subscription license. Instead, you must migrate data from the existing FMG-VM to a new FMG-VM with subscription license.

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 6.4.8.

FortiManager uses port TCP/4443 to connect to the Fortinet registry and download MEAs. Ensure that the port is also open on any upstream FortiGates. For more information about incoming and outgoing ports, see the FortiManager 6.4 Ports and Protocols Guide.

Supported models for MEA

You can use any of the following FortiManager models as a host for management extension applications:

FortiManager	FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, FMG-3900E, and FMG-4000E.
FortiManager VM	FMG-VM64, FMG-VM64-Ali, FMG-VM64-AWS, FMG-VM64-AWSOnDemand, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

Minimum system requirements

Some management extension applications supported by FortiManager 6.4.8 have minimum system requirements. See the following table:

Management Extension Application	Minimum system requirement
SD-WAN Orchestrator	At least 12GB of memory is recommended to support SD-WAN Orchestrator MEA.
Wireless Manager (WLM)	A minimum of 4 CPU cores and 8 GB RAM is typically required. Depending on the number of running applications, the allocated resources should be increased.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.4.8.

View Mode is disabled in policies when policy blocks are used

When policy blocks are added to a policy package, the *View Mode* option is no longer available, and policies in the table cannot be arranged by *Interface Pair View*. This occurs because policy blocks typically contain multiple policies using different incoming and outgoing interfaces, however, *View Mode* is still disabled even when policy blocks respect the interface pair.

Custom signature filenames

Custom signature filenames are limited to a maximum of 50 characters because FortiManager appends the VDOM suffix to custom signature filenames when FortiGate uses VDOMs.

SDN fabric connectors

According to the current design, SDN fabric connectors are installed on all FortiGates in an ADOM, even if the fabric connectors are not in use. See also bug ID 496870 in Known Issues on page 47.

Workaround: Place FortiGates in another ADOM when you do not want to install SDN fabric connectors to the devices.

ADOM version enforcement

Starting in FortiManager 6.4.6, ADOM versions are enforced. ADOM version N and N+1 are allowed, and the enforcement affects policy package installation.

For example, if you have ADOM version 6.0, and it contains a FortiGate running FortiOS 6.4, you cannot install a version 6.0 policy package to the FortiGate. The policy package installation fails with the following error message: `Device preparation failed: version mismatched,adom:6.0; dev:6.4.`

Management Extension Applications (MEA) and upgrade

Upgrading FortiManager when Management Extension Applications (MEA) are enabled may reset your *System Settings* to the default settings.

To prevent your *System Settings* from being lost, please disable all Management Extension Applications (MEA) prior to upgrading FortiManager.

Policy Hit Count on unused policy

FortiManager 6.4.3 and later no longer displays policy hit count information on the *Policy & Objects* > *Policy Packages* pane. However, you can view hit count information by using the *Unused Policies* feature and clearing the *Unused Only* checkbox. For more information, see the FortiManager 6.4 New Features Guide.

Wireless Manager (FortiWLM) not accessible

If Wireless Manager was enabled in FortiManager 6.4.0, you can no longer access it in the FortiManager GUI when you upgrade FortiManager to 6.4.2. When you try to access FortiWLM, you are redirected to the FortiManager dashboard.

SD-WAN Orchestrator not accessible

If SD-WAN Orchestrator was enabled in FortiManager 6.4.1, you can no longer access it in the FortiManager GUI after upgrading to FortiManager 6.4.2.

To workaround this issue, run the following CLI command to manually trigger an update of SD-WAN Orchestrator to 6.4.1 r2:

```
diagnose docker upgrade sdwancontroller
```

Support for FortiOS 6.4 SD-WAN Zones

In 6.4 ADOMs, SD-WAN member interfaces are grouped into SD-WAN zones. These zones can be imported as normalized interfaces and used in firewall policies.

Customers upgrading FortiGates from FortiOS 6.2 to 6.4 who cannot upgrade the ADOM are advised to temporarily disable SD-WAN central management until they can upgrade the ADOM to 6.4. This is to prevent FortiManager from attempting to delete the newly created SD-WAN zones on the FortiGate.

FortiGuard Rating Services with FortiGate 6.4.1 or Later

FortiManager 6.4.1 or later is the supported version to provide FortiGuard rating services to FortiGate 6.4.1 or later.

Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FMG-VM64-XEN image is larger than 128M. Before updating to FortiManager 6.4, increase the size of the ramdisk setting on Citrix XenServer.

To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:
   ```
   xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
   ```
2. Confirm the setting is in effect by running `xenstore-ls`.
   ```
   ----------------------
   limits = ""
   pv-kernel-max-size = "33554432"
   pv-ramdisk-max-size = "536,870,912"
   boot-time = ""
   ---------------------------
   ```
3. Remove the pending files left in `/run/xen/pygrub`.

The ramdisk setting returns to the default value after rebooting.

Multi-step firmware upgrades

Prior to using the FortiManager to push a multi-step firmware upgrade, confirm the upgrade path matches the path outlined on our support site. To confirm the path, please run:

```
dia fwmanager show-dev-upgrade-path <device name> <target firmware>
```

Alternatively, you can push one firmware step at a time.

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
set ssl-protocol t1sv1
end
```

Upgrade Information

You can upgrade FortiManager 6.2.0 or later directly to 6.4.8.

For other upgrade paths and details about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*.

This section contains the following topics:

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. In addition the local password is erased.

A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}
execute format {disk | disk-ext4 | disk-ext3}
```

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Aliyun

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FMG_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

Microsoft Hyper-V 2016 is supported.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

For more information see the FortiManager Data Sheet available on the Fortinet web site. VM installation guides are available in the Fortinet Document Library.

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

Product Integration and Support

This section lists FortiManager 6.4.8 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

FortiManager 6.4.8 support

This section identifies FortiManager 6.4.8 product integration and support information:

To confirm that a device model or firmware version is supported by the current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```

Always review the Release Notes of the supported platform firmware version before upgrading your device.

Web browsers

This section lists FortiManager 6.4.8 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 91
- Google Chrome version 92

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS/FortiOS Carrier

This section lists FortiManager 6.4.8 product integration and support for FortiOS/FortiOS Carrier:

- 6.4.0 to 6.4.9
- 6.2.0 to 6.2.10
- 6.0.0 to 6.0.14

FortiADC

This section lists FortiManager 6.4.8 product integration and support for FortiADC:

- 6.0.1
- 5.4.4

FortiAnalyzer

This section lists FortiManager 6.4.8 product integration and support for FortiAnalyzer:

- 6.4.0 and later
- 6.2.0 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiAuthenticator

This section lists FortiManager 6.4.8 product integration and support for FortiAuthenticator:

- 6.0. to 6.3
- 5.0 to 5.5
- 4.3

FortiCache

This section lists FortiManager 6.4.8 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

FortiClient

This section lists FortiManager 6.4.8 product integration and support for FortiClient:

- 6.4.0 and later
- 6.2.1 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiDDoS

This section lists FortiManager 6.4.8 product integration and support for FortiDDoS:

- 5.4.2
- 5.3.1
- 5.2.0
- 5.1.0
- 5.0.0
- 4.7.0
- 4.6.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3

Limited support. For more information, see Feature support on page 20.

FortiMail

This section lists FortiManager 6.4.8 product integration and support for FortiMail:

- 6.4.0 and later
- 6.2.0 and later
- 6.0.10 and later
- 5.4.12
- 5.3.13

FortiSandbox

This section lists FortiManager 6.4.8 product integration and support for FortiSandbox:

- 4.0.2
- 3.2.2
- 3.1.4
- 3.0.6
- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2

FortiSOAR

This section lists FortiManager 6.4.8 product integration and support for FortiSOAR:

- 6.4.0 and later
- 6.0.0 and later

FortiSwitch ATCA

This section lists FortiManager 6.4.8 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

FortiTester

This section lists FortiManager 6.4.8 product integration and support for FortiTester:

- 3.9
- 3.8
- 3.7

FortiWeb

This section lists FortiManager 6.4.8 product integration and support for FortiWeb:

- 6.3.15
- 6.2.5
- 6.1.2
- 6.0.7
- 5.9.1
- 5.8.6
- 5.7.2
- 5.6.1
- 5.5.6
- 5.4.1

Virtualization

This section lists FortiManager 6.4.8 product integration and support for virtualization:

- Amazon Web Services (AWS)
- Citrix XenServer 6.0+ and Open Source Xen 4.1+
- Linux KVM
- Microsoft Azure
- Microsoft Hyper-V 2008 R2, 2012, 2012 R2, 2016, and 2019
- VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7, and 7.0
- Nutanix AHV (AOS 5.10.5)
- Google Cloud (GCP)
- Oracle Cloud Infrastructure (OCI)
- Alibaba Cloud (AliCloud)

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiADC		✓		
FortiAnalyzer			✓	✓
FortiAuthenticator				✓
FortiCache			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSOAR		✓		
FortiSwitch ATCA	✓			
FortiWeb		✓	✓	✓
Syslog				✓

Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiManager, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiManager. For more information, see the *FortiAnalyzer Administration Guide*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 6.4.8.

Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

This section contains the following topics:

FortiGate models

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate 6000 Series:** FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F, FortiGate-6300F-DC, FortiGate-6301F-DC, FortiGate-6500F-DC, FortiGate-6501F-DC **FortiGate 7000 Series:** FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7000F, FortiGate-7121F **FortiGate DC:** FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC **FortiGate Hardware Low Encryption:** FortiGate-100D-LENC **FortiWiFi:** FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F **FortiGate VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV,FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen **FortiGateRugged:** FortiGateRugged-60F, FortiGateRugged-60F-3G4G	6.4

Model	Firmware Version
FortiGate: FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FortiGate-60E-POE, FortiGate-61E, FortiGate-60F, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-100F, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1100E, FortiGate-1101E, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate 6000 Series:** FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F, FortiGate-6300F-DC, FortiGate-6301F-DC, FortiGate-6500F-DC, FortiGate-6501F-DC **FortiGate 7000 Series:** FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7000F, FortiGate-7121F **FortiGate DC:** FortiGate-80C-DC, FortiGate-401E-DC, FortiGate-600C-DC, RortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC **FortiGate Hardware Low Encryption:** FortiGate-80C-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC **FortiWiFi:** FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE **FortiGate-VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager **FortiGate Rugged:** FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	6.2

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-GBL, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FortiGate-60F, FortiGate-61F, FG-60F, FG-61F, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FortiGate-100F, FortiGate-101F, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FortiGate-2200E, FortiGate-2201E, FG-2500E, FortiGate-3300E, FortiGate-3301E, FG-3000D, FG-3100D, FG-3200D,FortiGate-3600E, FortiGate-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E **FortiGate 5000 Series:** FG-5001D, FG-5001E, FG-5001E1 **FortiGate 6000 Series:** FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F, FortiGate-6300F-DC, FortiGate-6301F-DC, FortiGate-6500F-DC, FortiGate-6501F-DC **FortiGate 7000 Series:** FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7000F, FortiGate-7121F **FortiGate DC:** FG-401E-DC, FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3600E-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC **FortiGate Hardware Low Encryption:** FG-100D-LENC, FG-600C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list. **FortiWiFi:** FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-40F, FWF-40F-3G4G, FWF-41F, FWF-41F-3G4G, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate VM:** FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP,VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	6.0

FortiGate special branch models

The following FortiGate models are released on a special branch of FortiOS. FortiManager supports these models.

Model	Firmware Version
FortiGate: FortiGate-200F, FortiGate-201F, FortiGate-1800F, FortiGate-1801F, FortiGate-2600F, FortiGate-2601F, FortiGate-3500F, FortiGate-3501F, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F **FortiGate DC:** FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC	6.4

Model	Firmware Version
FortiGate: FortiGate-30E-3G4G-GBL, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-200F, FortiGate-201F, FortiGate-1800F, FortiGate-1801F, FortiGate-2600F, FortiGate-2601F, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F **FortiGate DC:** FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, 4400F-DC, FortiGate-4401F-DC **FortiGate Rugged:** FortiGateRugged-90D **FortiWiFi:** FortiWifi-60E-DSL, FortiWiFi-60E-DSLJ,	6.2
FortiGate: FortiGate-30E-3G4G-GBL, FortiGate-41F, FortiGate-41F-3G4G, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60F, FortiGate-61F, FortiGate-600E, FortiGate-601E, FortiGate-1800F, FortiGate-1801F, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E **FortiGate DC:** FortiGate-1100E-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-3400E-DC, FortiGate-3401E-DC **FortiGate VM:** FortiGate-VM64-RAXONDEMAND **FortiWiFi:** FortiWiFi-41F, FortiWiFi-41F-3G4G,	6.0

FortiCarrier models

Model	Firmware Version
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3400E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier 6000 Series:** FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC **FortiCarrier 7000 Series:** FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7000F, FortiCarrier-7121F **FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier 6000 Series:** FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC	6.2

Model	Firmware Version
FortiCarrier 7000 Series: FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7000F, FortiCarrier-7121F **FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E **FortiCarrier 6000 Series:** FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC **FortiCarrier 7000 Series:** FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7000F, FortiCarrier-7121F **FortiCarrier-DC:** FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC **FortiCarrier-VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	6.0

FortiADC models

Model	Firmware Version
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	6.0
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	5.4

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E	6.4

Model	Firmware Version
FortiAnalyzer VM: FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand,FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	
FortiAnalyzer: FAZ-200F, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000E, FAZ-2000E, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.2
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.0
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	5.6
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B. **FortiAnalyzer VM:** FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	6.0 to 6.3
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000B, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	5.0 to 5.5
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	4.3

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E **FortiCache VM:** FCH-VM64, FCH-KVM	4.0, 4.1, 4.2

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-200B, FortiDDoS-400B, FortiDDoS-600B, FortiDDoS-800B, FortiDDoS-900B, FortiDDoS-1000B, FortiDDoS-1200B, FortiDDoS-1500E, FortiDDoS-2000B, FortiDDoS-2000E	5.2, 5.3
FortiDDoS: FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-1500B, FI-2000B, FI-2000E	5.1
FortiDDoS: FI-1500E, FI-2000E	5.0
FortiDDoS: FI-200B, FI400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.7

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM	6.4
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM	6.2
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM	6.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E **FortiMail Low Encryption:** FE-3000C-LENC	5.4
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B **FortiMail Low Encryption:** FE-3000C-LENC **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E **FortiProxy VM:** FPX-KVM, FPX-VM64	1.0, 1.1, 1.2

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000F, FSA-2000E, FSA-3000E, FSA-3000F **FortiSandbox-VM:** FSA-AWS, FSA-VM	4.0
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox-VM:** FSA-AWS, FSA-VM	3.2
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox-VM:** FSA-AWS, FSA-VM	3.1
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-AWS, FSA-VM	3.0
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D	2.5.2

Model	Firmware Version
FortiSandbox VM: FSA-KVM, FSA-VM	
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-VM	2.4.1 2.3.3
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D **FortiSandbox VM:** FSA-VM	2.2.0

FortiSOAR models

Model	Firmware Version
FortiSOAR VM: FSR-VM	6.4
FortiSOAR VM: FSR-VM	6.0

FortiSwitch ATCA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-5913C	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3.0 4.2.0

FortiTester models

Model	Firmware Version
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL	3.9
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL	3.8
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL	3.7

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-400C, ortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.2, 6.3
FortiWeb: FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XenServer	6.1
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-600D, FWB-1000D, FWB-1000E, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVER	6.0
FortiWeb: FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.9
FortiWeb: FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6

Model	Firmware Version
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV	5.4

Resolved Issues

The following issues have been fixed in 6.4.8. For inquires about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
691540	*Where Used* should indicate that an AP is still in used in one or more FortiGate devices.
697444	SSID with MPSK may not pass verification during an install.
718464	Firmware upgrade fails for FortiAP 421E from FortiManager.
726287	Deleting Floor Map may return a blank pop-up with error.
728372	Importing SSID with optional VLAN ID set creates incorrect per-device mapping.
750255	FortiManager should enable DFS channels on WTP profiles for FAP234F and FAP231F with region N.
750458	AP Manager should not send `local-authentication` for VAP with `wpa-enterprise` and Radius to managed FortiGate.
757706	FortiManager might downgrade FortiAP with enforced firmware version.
763233	AP profile may not contain SSID when AP Manager is in central management mode.
770234	5GHz DFS channels on AP Profile were not supported for FAP U231F.
772194	FortiManager should not install the setting `set security-redirect-url` without making any such change.
772213	FortiManager may try to delete default wtp 11ac-only profile on FortiWiFi-60F causing install to fail.
785471	FortiManager was deleting `wireless-controller` wtp and the objects referenced by wtp during the first installation after the upgrade.

Device Manager

Bug ID	Description
545239	After adding FortiAnalyzer fabric ADOM to FortiManager, *Device Manager*'s *Log Status*, *Log Rate*, or *Device Storage* columns cannot get data from FortiAnalyzer.

Bug ID	Description
587404	FortiManager sets incorrect `captive-portal-port` value when installing v6.0 policy package to v6.2 devices.
638750	*Where Used* may not work for IPsec Phase 2 allowing users to delete used objects.
662095	FortiManager may take too much time to send SLA updates to one thousand or more FortiGate devices.
673008	SD-WAN Rules order changes to the default order when creating a rule and moving it to the top.
677836	The *Client Address Range* setting should allow users to configure `assign-IPs` from firewall address or group.
691611	When FortiManager performs `auto-retrieve`, it causes all policy package statuses to become *unknown* after a new VDOM is created on FortiGate.
699893	SD-WAN's `priority-members` is missing from *CLI configuration* page.
701348	Once VRPP instance is created, user should be able to edit or delete it.
709214	System template should allow source interface to be selected when *specify* is activated as `interface-select-method`.
712578	FortiManager does not allow WiFi SSID with special characters.
713833	It may not be possible to rename device zone.
725334	Importing policy package shows `ngfw-mode policy-based` with the `inspection-mode` set to `proxy`.
726721	Unable to add multiple DNS domain names in *Provisioning Template*.
727123	*Meta Field* is not translating values with spaces into correct scripts.
729301	A managed FortiGate with assigned CLI template remains in *modified* state following a successful device configure installation.
729413	FortiManager is missing peer options with dial up user configuration with VPN IPSec Phase 1.
730482	CLI Template cannot add system DNS database entries if *set domain* contains the underscore character ("_").
731204	FortiManager may incorrectly display *Object already exists* message while creating a new Hardware Switch interface.
732246	Clock format option no longer works to format date in TCL scripts.
733379	FortiManager cannot edit global level configuration when management VDOM is not in the current ADOM.
733934	During zero-touch-provisioning with *Enforce Firmware Version* enabled, upgrade task may hang if the connection is reset during the image transfer.
735360	When editing a device group, search results do not show the device if VDOM name is matched by search keyword first.

Bug ID	Description
735402	Create a new CLI Group Template and try to add members to the CLI Group Template, but it does not allow users to select other *CLI Group Templates* that are already created.
737025	*SD-WAN monitor* widget may not be loaded when multiple performance SLAs are added.
737908	The install fails with *verification failure* displaying when trying to delete the LAN interface members.
739369	When revision history is large, FortiManager may be unable to retrieve configuration.
740893	Secondary IP may be purged when setting a description to VLAN interface.
743102	*Device & Groups* > *VPN Phase1/Phase2* does not show the *proposal* column when using FGT-VM type "FGVMIB".
743112	*Interface Bandwidth* widget on FortiManager under *Device Manager* does not display any data for FortiGate.
743267	FortiManager's GUI does not show the *virtual-switch* ports as interface members for Hardware switches.
744628	After exporting system template, importing the same configuration through the CLI may fail.
744973	FortiManager GUI throws an error when switching from *Policy & Objects* to *Device Manager*.
747955	There may be performance issue when onboarding new SD-WAN devices.
748240	When FortiAnalyzer is managed by FortiManager, new devices that are registered to FortiManager should be synchronized under the corresponding ADOM on FortiAnalyzer.
749823	*Named Address Static Route* with SD-WAN cannot be selected on FortiManager.
749923	SD-WAN logs cannot be saved for some devices when `sdwan-monitor-history` is set as `enabled`.
750303	Under *System* > *Interface*, the data shown on this page may be incomplete.
750838	FortiManager may fail to import device list from another FortiManager due to the meta field containing prefix "_meta_".
751427	Provisioning Template with empty name cannot be deleted or edited.
753258	FortiManager may be unable to show SD-WAN monitor data when the rtmmond daemon is stuck.
754465	FortiManager should also count promoted hidden devices.
755519	Zero-touch provisioning with script installation may fail due to duplicated `snmp-index`.
759905	When creating a device zone, device mapping may not be created when the zone is mapped to a normalized interface with the *map as zone only* option.
760099	When creating EMAC VLAN from *Device Manager,* FortiManager should show *VLAN ID* field.
760132	Device Manager may be unable to delete FortiGate-7000E HA cluster members.

Bug ID	Description
762082	When creating a Static Route, FortiManager may take a few seconds to display available *Named Address*.
763797	Installation fails due to configuring `forward-error-correction` on FGT's interfaces.
764491	Unable to configure more than one IP addresses for `vrdst` under the `interface vrrp` setting.
764841	FortiManager is unable to use secondary IP as source IP in DNS database.
765762	FortiManager is unable to install the switch controller > VLAN interface configuration during the ZTP process.
773336	FortiToken provision button is grayed out in *Device Manager* while it is enabled on FortiGate with the same token.
777925	Several unregistered FGTs consume FortiManager's resources. As a result, FMG becomes very slow and unresponsive.
779260	When `sdwan-monitor-history` is enabled, replace *last 5 minutes* with *last 10 minutes*.
779836	FortiManager cannot install TCP-connect using Random port for SD-WAN.
779900	Administrative user GUI-dashboard information should be deleted upon VDOM deletion.
792553	Removing VLANs from Zone and adding a new VLAN to the same Zone deletes that Zone.
793941	Unable to install VPN psk with special characters through CLI template.
795913	*Error Probe Failure* has been observed when adding FortiAnalyzer to FortiManager.

FortiSwitch Manager

Bug ID	Description
684371	Clicking *OK* to import FortiSwitch Template results in no response.
748200	FortiSwitch monitor may show incorrect interface status for QSFP port.
764258	FortiManager should not update trunk-member value as it is controlled by FortiGate.

Global ADOM

Bug ID	Description
660852	FortiManager should not save invalid default value for `ssl-ssh-profile` in global database.
691562	Threat feeds global objects are not installed to destination ADOM when using the *assign all*

Bug ID	Description
	objects option.
725763	Automatic install to ADOM devices may fail from Global ADOM.
728803	Copying global firewall policy may fail due to duplicate IPS sensors.
737381	FortiManager should not allow users to delete the default reserved address object starting with "g-".
740942	*srcintf* selector in *Traffic Shaping Header* or *Footer Policy* may not work in Global ADOM.
741942	FortiManager should show clear error message for duplicated object assigned from Global ADOM.
745772	FortiManager may randomly delete FortiManager IPv4 policies when assigning from the Global ADOM.
760804	FortiManager may return an error when adding address object to global policy.
743734	Cannot remove objects from Global Database.
768527	After upgrading the global ADOM, installation failed due to the custom `ssl-ssh-profile` config.

Others

Bug ID	Description
505795	FortiManager should allow users to configure the list of allowed TLS cipher suites.
657997	Assigning device to system template may not work through JSON when FortiManager is in workspace mode.
707911	FortiManager should be able to assign VLAN interface to FortiExtender.
715601	Under some conditions, disk usage may reach 100% after a few days.
718251	Web service with port 8080 disabled may still be in listening state.
733078	FortiManager may show multiple fmgd crashes with signal 11 segmentation fault.
733208	Users may be unable to log in from GUI after restored database with changed HTTP or HTTPS port number.
738639	Users should be able to obtain status of the FGFM `reclaim-dev-tunnel` through an API call.
740523	Retrieve task may fail because the `autoupdate` file has already been deleted by FGFM.
742137	FortiManager may return an error when running an Ansible script to configure network interfaces, zones, and policies.

Bug ID	Description
744197	If a VDOM is created and then gets the VDOM information from JSON API, the VDOM mode may be shown as NULL.
744736	FGFM tunnel may go up and down with multiple fgfmsd crashes.
746311	`fgdsvr` process may crash when URL length is longer than 1024 characters.
750419	Execution of integrity check may remove dynamic mappings.
763635	Unable to upgrade an ADOM from 6.2 to 6.4.
763669	FortiManager Pay-As-You-Go should support connection to FortiCare through proxy.
764674	Map should use the region defined by the coordinates in *System Settings* > *Advanced Settings* or the FortiManager's time zone.
766105	FortiManager may be unable to upgrade ADOM from 6.2 to 6.4 due to cdb crash.
766874	FortiManager holds the wrong value for AP limit of the FG-80F.
775574	There is a *Criteria Latency* field which is different between FortiGate and FortiManager when creating the manual interface option for SDWAN rules.
776342	System NPU values may be different between FortiManager and FortiGate-1801F.
776413	FortiManagerlock/commit operation is very slow when FortiManager HA is enabled.
783226	*Fabric View* may keep loading.
792887	Verification fail for default dnsfilter profile due to wrongly install "set category 0".
794304	*Interface Bandwidth* widget is displayed in ADOM 6.2 in FortiManager version 6.4.

Policy and Objects

Bug ID	Description
503978	*Thread Feeds* should be *Threat Feeds* on *Fabric Connector*.
549492	Load-balance type VIP cannot be displayed and saved correctly.
585177	FortiManager is unable to create VIPv6 virtual server objects.
615250	Search by CVE may not work for both IPS signatures and IPS filters.
644822	Imported SDN connector objects may change to random names.
657534	SSH and MAPI should not be supported in file filter profile protocol under flow mode.
696367	Hit count, first used, and last used may not get updated on FortiManager.
699975	Multiple filters are missing for Azure SDN connector.
701750	The *App Control* set to *Monitor* in FMG causes the app to disappear from FGT.

Bug ID	Description
709908	When checking the status on AntiVirus profile, it may not show the correct inspection mode in list view when status stays in *flow-based (Full Scan)*.
713886	FortiManager returns error *method failure*, when setting a shaping profile in normalized interface using per-device mapping.
714375	There is no warning messages when assigning in-use normalized interfaces.
717031	FortiManager doesn't update the *Hit Count* number.
718223	Hyperscale firewall EIF shall not be enabled when IP pool with CGN overload configuration is used in a policy.
725024	*Proxy Policy* page shows empty when the *View Mode* is selected as *Interface Pair View*.
725132	When modifying IP address of *Default VPN Interface* of spoke in Device Manager, hub remote gateway should be modified to reflect that change.
726328	SSL-SSH profile may display incorrect options when using SSL certificate inspection.
729705	Installing policy requires interface validation for interfaces not being used in the policy package.
730523	Unused policies tool may always generate a PDF containing all policies.
731053	FortiManager may miss some *Internet Service* entries.
732138	Non-full admin users should be able to export *Policy Check* and *Unused Policy* results.
732199	FortiManager displays the group ID instead of displaying name with NSX-T Connector.
734556	FQDN type firewall address object can be created with an unsupported format.
737424	Policy package import fails due to the *Device mapping::"query failed.* error.
738475	Special characters within policy's comment causes all policies to disappear from the GUI.
740944	Custom IPS signature script may fail to run on policy package or ADOM database.
742257	NPU log servers for hyperscale does not show up in policy package.
744049	Proxy policy does not accept configuration with both IPv4 and IPv6 address objects.
744591	Installing or importing IPS custom signature may fail when a signature's name contains a space character.
744766	FortiManager may not be able to retrieve IP address for group with NSX-T v3.1.2.
744934	FortiManager may try to install undesirable changes to FortiGate-5001E, FortiGate-5001E1, and FortiGate-5001D.
745355	Section labels are not visible in *virtual-wire policy* section.
745884	FortiManager GUI may not respond when triggering policy package install wizard under *Policy & Objects*.
746273	Column filter may be extremely slow with large policy package.
747537	*Where Used* should show the correct object references for newly cloned objects.

Bug ID	Description
747558	FortiManager filters should work for *Hit Counters*, *First Session*, and *Last session*.
748222	Cloning of a policy package is grayed out for admin users with restricted access to particular policy packager folder.
748235	Filtering by hit count may not work for policies.
748246	*Where Used* may result an empty top-left frame for policy packages.
748467	FortiManager does not have the same profiles as FortiGate with explicit proxy policy.
748498	There may be issue with *Transparent Web Proxy* when using interface pair view.
748556	FortiManager should not allow users to create Explicit proxy FTP with pool name.
749519	IPv4 policies in policy block may be hidden on FortiManager's GUI.
749576	FortiManager may try to install hidden `synproxy` parameters for DOS policy to FortiGate.
750160	`custom-url-list` may not be correctly parsed when URLs contain space characters.
750539	If FortiGate allows selecting *LogMeIn* app using specific filter override, FortiManager should also allow it.
750882	User may not be able to save changes in SSL/SSH inspection profile from GUI.
751137	Installation performance issues may occur with a large number of dynamic mappings and many FortiAP or FortiSwitch devices.
751710	Editing a global user FSSO object's dynamic mapping is not possible.
751767	Export to Excel when filters are applied for a policy package does not work.
752777	FortiManager should be able to manage valid authentication rules containing *User-Agent* proxy address.
752822	FortiManager may not respond when adding a firewall address or group to a policy and changing the policy comment at the same time.
754225	Policy package status is out of sync without changes.
755252	Plus (+) sign should be added for SMS phone number when two-factor FortiToken Cloud is enabled.
755348	FortiManager should support more than one thousand traffic shapers.
757164	FortiManager database contains parameter `webfilter-searchengine-Baidu-gb2312` that does not exist on FortiGate.
758526	FortiManager should be able to delete many per-device mappings quickly.
758809	When policy package in policy-based NGFW mode, FortiManager may still set action to accept, even when the policy is specified as deny.
760869	Deleted objects may remain referenced in firewall policy.
765709	FOS 6.4.9 syntax support.

Bug ID	Description
765793	Adding custom signature with *_vdom-name* should not prevent pushing changes to numerous devices.
765812	Hyperscale policy packages do not show log server until you get into a policy.
767317	Policy Hit Count may not be updated for Read-Only admin.
768353	Commit action is taking too much time and it makes the FortiManager slow.
769997	Selection for user SAML as member under the user group may not take effect.
770210	*Where Used* may not report used objects properly.
770256	FortiManager displays error when using *push to install* for objects utilized by policy blocks .
770678	Changing *Action* from *Accept* to *Deny* should ignore all UTM profiles within the firewall policy.
771941	FortiManager is unable to import or create virtual server with real servers using the same IP but different `http-host`.
774435	Right-click menu to add object may return an error: *cgn-resource-quote:out of range*.
775128	Unable to create more than twenty (20) SAML users in policy package object.
776361	Policy lookup may not work if the managed devices are in transparent mode.
777554	There may be slowness when using *Find Duplicate Objects* with *Merge* tools.
779947	Address group changes for per-device mapping do not apply to FortiGate when address group is used in policy route.
779965	Users may be unable to export firewall header and footer policies to Excel.
783899	There may not be empty lines in *IPS Signature and Filters*.
786684	Installation fails because the *virtual-wan-link* did not exist.
789957	Created time doesn't indicate AM or PM on the *Tools* > *Find Unused Policies*.
791797	Installation failed after upgrading ADOM from 6.2 to 6.4.

Revision History

Bug ID	Description
618305	FortiManager changes configuration system csf settings.
643101	Copy may fail due to VIP overlapping when installing policy package.
657424	FortiManager may disable the "l2forward" and "stpforward" settings on virtual switch interface when installing policy package.
660525	When installing from FortiManager, it may unset comment, organization, and subnet-name during install.

Bug ID	Description
674094	FortiManager may unset explicit proxy's HTTPS and PAC ports and change the value to 0 instead.
674196	Installation may fail after edited or created a firewall policy if reputation-minimum is set.
691240	FortiManager should not unset the value forward-error-correction with certain FortiGate platforms.
700495	FortiManager 6.2 ADOM may be sending set synproxy to FortiGate-1801F.
713552	If VIP address's source-filter list is too long, installation may fail.
722604	After removed a member of user group that is used only in XAUTH, FortiManager is not deleting the unused local user on FortiGate.
724647	After upgraded to 6.4, retrieve from a chassis may take a long time.
725252	When customer is trying to push policy package to a device group, installation window may not show any progress but a red cross.
725557	Install always try to delete hardware switch member interface causing installation failure.
725717	After upgrade, installation may fail due to mcast-session-counting.
728447	Installation may fail due to VIP's mapped IP as a range with two identical IP addresses.
728918	FortiManager should install changes applied on Global policy package and not indicate warnings like "no installing devices/no changes on package".
729148	Install fails when new transparent mode VDOM is added directly via FortiGate CLI and imported into FortiManager.
735455	FortiManager may try to delete thousands of policies during install.
740858	GCP project name must be set during install.
741543	Install may fail with unset MAC address on EMAC VLAN.
742806	When modifying a configuration and installing Device Setting only , FortiManager may not display the device's configuration change.
744966	After upgraded FortiManager, policy install verification may fail with Config status changes to Conflict due to invalid default value for log memory filter.
745715	FortiManager may not be able to install policy package with firewall rule using VIP group due to zone binding.
747837	FortiManager may try to delete interfaces lan1, lan2, and lan3 which are used by virtual-switch.sw0 on FortiGate-40F.
748350	Explicit proxy FTP ssl-ssh-profile application-list may not be installed.
748462	FortiManager should not set the HA interface IP under the central-management on FortiGate when the master unit fails.
749587	If a device revision is corrupted, FortiManager may be able to remove or create any revision.

Bug ID	Description
750637	FortiGate-5001E, FortiGate-5001E1, and FortiGate-5001D may be mistakenly set to support switch-profile.
751771	Users may not be able to create hardware switch interface from FortiManager.
751776	Renaming IPSec Phase1 that is member of a zone causes all zone related rules to be re-created.
754081	Application Control signatures belong to Industrial Category are removed from FortiGate in split mode during policy install.
755059	After disabled NAT on hyperscale policy, there may be installation failure on unset action.
755687	FortiManager may show admin with no password when adding a new VDOM to FortiGate-2200E/2201E.
756508	FortiManager may unset chassis ID causing HA cluster lost.
757716	There may be install issue with Web Filter's "config ftgd-wf" which does not exist on NGFW policy mode on FortiGate.
764497	FortiManager should not create a new wildcard FQDN object while renaming it.
767824	FortiManager may unexpectedly delete custom signature when installing policy package.

Script

Bug ID	Description
384139	Filter does not work on device group.
654700	Users need to open "View Script Execution History" to see that TCL script fails.
740938	Direct CLI script may fail when it contains an 'exec' command.
757156	When running CLI script remotely on 100+ firewalls, partial configuration is retrieved and it may cause routing to be removed from device database.
780604	When creating a new phase1 interface, dpd=on-idle settings may not be saved.
787113	TCL scripts fails to run if the admin's password is longer than 36 characters.

Services

Bug ID	Description
644021	FortiManager should be able to use custom certificates for update-related services.

Bug ID	Description
704584	FortiAP firmware may not be listed and cannot be imported.
718256	FMG-VM64-AWSOnDemand may not retrieve the proper license when it is behind a proxy.
725118	FortiManager may not log FortiGuard connectivity failures.
741846	AP upgrade task may hang at 45%.
748489	Numerous *svc cdb reader* processes reaching 100% CPU utilization.
796345	FMG does not recognize the entitlement file for some FGTs.

System Settings

Bug ID	Description
640670	If a user specified ADOMs, including global ADOM, workflow approval may not be able to find the same user.
687992	Backup that includes IPSec VPN cannot be restored.
690926	FortiManager is removing SD-WAN field description upon ADOM upgrade from 6.2 to 6.4.
696554	FortiManager may generate a lot of *cdb event log for object changed* event logs.
706303	Template assignment or save may not generate clear event logs.
721153	Scroll bar is missing from device drop-down list on ADOM overview page.
727233	ADOM license count should not count root ADOM.
728991	Nested group search fails with `Bad search filter`, if the user DN contains characters like "," and "()".
729280	Admin User with no access to management ADOM or VDOM can create a new VDOM from non-management ADOM > VDOM.
731084	FortiManager upgrade should not have warning when there is no upgrade path.
734422	The "svc sys" daemon may have high memory usage when API is used to upgrade FortiGate devices.
735067	When creating a local account with the *Force this administrator to change password upon next log on* option selected, the setting should be applied for the first login.
737142	FortiManager should support using the special character "@" in SNMP community name.
738622	ADOM upgrade from 6.0 to 6.2 may fail due to FortiExtender object.
745333	Remote authentication servers should not be synchronized among HA members.
745365	Event log may be truncated when the log contains many address objects.
746568	FortiManager may continuously change NTP synchronization server.

Bug ID	Description
748237	Users may be unable to disable ADOM using GUI or CLI.
751069	User may be unable to disable ADOM after upgrade.
762708	LDAP may become stuck for twenty seconds if LDAP is not responding.
768682	Setting a Cluster ID for a model HA cluster results in an invalid group ID under `config system ha`.
775091	Two factor authentication fails when special characters are used in CN.
777726	FortiManager may not generate event logs for meta field changes.
778405	Script Groups should be copied with their members when cloning an ADOM.
783066	If the number of FortiGate devices registered is in the upper limit of the license count, it may cause HA to become asynchronized.
790409	`idle_timeout` under admin settings is not converted properly after performing the upgrade.
795655	FortiManager loads the *Administrator* list under the *System Settings* very slowly.

VPN Manager

Bug ID	Description
721783	Applying Authentication or Portal Mapping changes may take several minutes.
735417	FortiManager may purge mac-addr-check-rule when installing to FortiGate.
748488	Cloned VPN Phase1 interface may have several different parameters than the original interface.
750227	Removing a spoke or hub from VPN community may result in partial configuration removal.
774040	`keyboard-layout` configuration in VPN SSL web portal predefined RDP bookmark generates incorrect commands.
779498	VPN monitor may not display correct information when FortiManager is in advanced ADOM mode.
780154	Policy package should be pushed to VPN hubs without error *interface IP is 0*.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
770575	FortiManager 6.4.8 is no longer vulnerable to the following CVE-Reference: • CVE-2022-22300

Known Issues

The following issues have been identified in 6.4.8. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
794836	AP Manager forces PMF disable with any WPA2 Security Mode.
794836	Protected Management Frames (PMF) feature always gets disabled when security mode is set to *WPA2 (Enterprise or Personal)*.

Device Manager

Bug ID	Description
676415	SAML account with remote certificate not getting imported to FortiManager-Cloud.
704106	Certificate enrollment fails using SCEP on Microsoft server with sub-ca certificate chains.
762650	FortiManager is sending commands which do not exist in FortiGates; issue happens only on 80/81F and 60F.
775552	The *View Device Revision* under *Revision History* does not display the full and complete device configuration.
806622	Installation failed after configuring the link-monitor.

Others

Bug ID	Description
729175	FortiManager should highlight device consisting of specific IP address under *Fabric View*.
792296	ADOM upgrade fails due to the virtual wire pair policy.
804244	ADOMs created by XML API cannot be locked or unlocked.

Policy & Objects

Bug ID	Description
652753	When an obsolete internet service is selected, FortiManager may show entries IDs instead of names.
656991	FortiManager should not allow VIP to be created with same IP for External IP and Mapped IP Address.
706809	Policy Check export does not have the last hit count details anymore.
726105	CLI Only Objects may not be able to select FSSO interface.
731037	There may be File Filter file type mismatch between FortiGate and FortiManager.
758680	Unable to complete the Cisco pxGrid fabric connector's configuration on FortiManager.
765154	Installation fails when trying to disable the "safe search" on existing DNS filter from FortiManager.
767255	FortiManager fails to install the custom signature because it is too long.
773249	FortiManager may not display the correct number of firewall address objects while adding the objects to DoS policy.
773403	FortiManager may now differentiate between the ISDB objects "Predefined Internet Services" and "IP Reputation Database".
774058	Rule list order may not be saved under File Filter Profile.
791357	Installation failed when using `custom-deep-inspection`.
802934	FortiManager's Policy Package Diff displays policy objects as changed, even though there are no changes.
805783	After the 6.0 ADOM upgrade, installing the same v6.0 policy package gets *unset webfilter-profile* in wanopt proxy policy.
805966	Verification fails due to the `resource-limits.proxy`.
811450	The *Installation Preparation* step for installing the policy package to FortiGate takes a long time.

Revision History

Bug ID	Description
496870	Fabric SDN Connector is installed on FortiGate even if it is not in used.
779864	FortiManager cannot install ISDB object 'Microsoft-Intune'.

Services

Bug ID	Description
752849	FortiManager doesn't have the proper version string of FGT's IPGeo Info.
754038	Multi-step FortiGate firmware upgrades via FortiManager may break FortiGate HA cluster.
808121	FortiManager ignores `add_no_service` setting for Unauthorized Devices.

System Settings

Bug ID	Description
579964	FMG-VM64-Cloud needs to provide GUI support for ADOM upgrade in system information dashboard.
811633	Restricted Administrators using the API requests have full R/W access.

VPN Manager

Bug ID	Description
615890	IPSec VPN Authusergrp option "Inherit from Policy" is missing when setting xauthtype as auto server.
784385	FortiManager causing faulty dynamic mapping for VPN manager interface during policy package import. **Workaround**: In order to remove invalid mappings of VPNMGR interface, run the following command for the affected ADOM: `Diag cdb check policy-packages <ADOM>`
796104	FortiManager deletes and re-creates VPN routes with different IDs on every install.

Appendix A - FortiGuard Distribution Servers (FDS)

In order for the FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as a FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the items listed below:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through via port 443.

FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform/version:

Platform	Antivirus	WebFilter	Vulnerability Scan	Software
FortiClient (Windows)	✓	✓	✓	✓
FortiClient (Mac OS X)	✓		✓	
FortiMail	✓			
FortiSandbox	✓			
FortiWeb	✓			

To enable FortiGuard Center updates for FortiMail version 4.2 enter the following CLI command:

```
config fmupdate support-pre-fgt-43
set status enable
end
```

Appendix B - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiManager hardware models and virtual machines.

Hardware models

The following table identifies the default number of ADOMs supported for FortiManager hardware models G series and later. It also identifies the hardware models that support the ADOM subscription license and the maximum number of ADOMs supported.

FortiManager Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
3000G Series	4000	✓	8000

For FortiManager F series and earlier, the maximum number of ADOMs is equal to the maximum devices/VDOMs as described in the FortiManager Data Sheet.

Virtual Machines

FortiManager VM subscription license includes five (5) ADOMs. Licenses are non-stackable. Additional ADOMs can be purchased with an ADOM subscription license.

For FortiManager VM perpetual license, the maximum number of ADOMs is equal to the maximum number of Devices/VDOMs listed in the FortiManager Data Sheet.